

**IN THE UNITED STATES DISTRICT COURT
SOUTHERN DISTRICT OF NEW YORK**

SECURITIES AND EXCHANGE)	
COMMISSION,)	
)	
Plaintiff,)	
)	Civil Action No. 1:23-cv-09518-PAE-BCM
v.)	
)	
SOLARWINDS CORP. and TIMOTHY G.)	
BROWN,)	
)	
Defendants.)	

**DECLARATION OF TIMOTHY BROWN IN SUPPORT OF
DEFENDANTS' MOTION FOR SUMMARY JUDGMENT**

I, Timothy Brown, hereby declare under penalty of perjury, pursuant to 28 U.S.C. § 1746, as follows:

I. INTRODUCTION

1. I am the Chief Information Security Officer (CISO) at SolarWinds Corporation (the “Company” or “SolarWinds”), a position I have held since 2021. Previously, from 2017 to 2021, I held the position of Vice President of Security and Architecture. I make this declaration in support of the motion for summary judgment of Defendants SolarWinds and myself (collectively, “Defendants”). The facts set forth herein are based on my personal knowledge and my review of the records of SolarWinds. If called upon to do so, I can and will competently testify to these facts.

2. I understand that the Securities and Exchange Commission (SEC) relies on certain documents and emails that I drafted, reviewed, or received during my tenure at the Company to infer that certain representations in the SolarWinds online Security Statement were false or misleading. I submit this declaration to explain my understanding of those documents and

specifically to clarify that the documents do not contradict the representations in the Security Statement at issue, which have been true throughout my tenure at SolarWinds.

II. DOCUMENTS CITED BY THE SEC

A. Documents on Which the SEC Intends to Rely to Challenge the Security Statement's Representations About Role-Based Access Controls

1. August 2017 Budget Proposal

3. I understand the SEC has cited a budget proposal I prepared in August 2017, soon after I joined the Company, and that it intends to rely on language in the document to challenge the Security Statement's representations about role-based access controls. Ex. A (SW-SEC00259782). I understand the SEC is focused on a bullet included next to the proposal, under "Risks of Non-Investment," stating: "Current state of security leaves us in a very vulnerable state for our critical assets. A compromise of these assets would damage our reputation and impact us financially." Ex. A (SW-SEC00259782 at -788).

4. I included this language alongside the budget request to underscore the general importance of investing in cybersecurity as part of a process of continuous improvement and to increase the likelihood that the budget request would be granted. I thought there was room for improvement in the Company's cybersecurity program, but beyond that, my comment was merely hyperbole to support a budget request.

5. Neither this language nor anything else in the budget request was intended to convey anything inconsistent with the Security Statement. In particular, the language was not intended to convey that we lacked role-based access controls, which we had in place ever since I arrived at the Company. If I was trying to communicate that SolarWinds lacked role-based access controls, I would have said so clearly—and through a different channel than making a budget request. That was not the case.

6. I also understand the SEC cites two other slide decks from late 2017 in which the same budget proposal from the August 2017 slide deck re-appears, with the same verbiage. This would have simply been the result of the same budget proposal being copied to other similar slide decks around this time, not because I was making any sort of repeated finding about SolarWinds' cybersecurity posture.

7. Finally, I understand the SEC cites the same language in a couple of slides I included in a draft slide deck I prepared in October 2018. Ex. B (SW-SEC00313351 at -361). Specifically, I included my original budget request from August 2017 in this slide deck, alongside a second copy of it labeled "Updated October 2018 with status," with the font color of some of the language changed to green, yellow, or red font. I made the font for the "Current state of security leaves us in a very vulnerable state for our critical assets" language yellow. All I was trying to convey by this was that the Company had made progress since August 2017, but that there was still work to do. While my supervisor, Rani Johnson, reviewed this draft slide deck, I do not recall whether it actually ended up being used to update management.

2. August 2019 NIST Scorecard

8. I understand the SEC has cited a NIST Scorecard prepared by Rani Johnson and myself that was included in an August 2019 Quarterly Risk Review ("QRR") presentation to management, and that the SEC intends to rely on language in the Scorecard to challenge the Security Statement's representations relating to role-based access controls. In particular, I understand that the SEC intends to rely on the "1" listed as the "NIST Maturity Score" for "Authentication, Authorization and Identity Management," and on a bullet at the top of the slide stating: "Access and privilege to critical systems / data is inappropriate. Need to improve internal processes | procedures." *See, e.g.*, Ex. C (SW-SEC0001497) at -507. Neither notation was meant to indicate that the Company lacked role-based access controls.

9. As Ms. Johnson explains in her declaration, which I have reviewed, our focus during the Relevant Period was on migrating to a new Identity and Access Management (“IAM”) solution—Microsoft Azure Active Directory (“Azure AD”). This project was aimed at improving our access-provisioning process by making it more automated and centralized at a technical level, which would reduce the risk of errors. Automation is a common way that companies mature their controls under NIST CSF. We were also working to roll out a Privileged Access Management (“PAM”) solution known as “Thycotic,” which provides specialized tooling to manage access to privileged accounts. However, irrespective of these improvements, we had access controls in place as the Security Statement described—they were just implemented through relatively manual processes. I have reviewed Ms. Johnson’s Declaration on this topic and agree with her statements. *See* R. Johnson Decl. ¶¶ 4-18.

3. September 2018 Slide Deck

10. I understand the SEC also intends to rely on a slide deck from September 2018, in which a slide in the appendix includes a notation in red font stating “Identity Management – Role and Privilege Management,” with a legend on the slide indicating that red font means “Limited or non existent.” Ex. D (SW-SEC00386134) at -6143.

11. Again, this notation was not about a lack of role-based access controls. It was about the limited IAM and PAM *tooling* we had in place at the time. The fact that we had not yet rolled out this tooling does not imply that we lacked role-based access controls as represented in the Security Statement.

B. Documents on Which the SEC Intends to Rely to Challenge the Security Statement’s Representations About Secure Software Development

12. I understand the SEC intends to rely on certain documents, which I helped prepare, to challenge the Security Statement’s representations about security testing of SolarWinds

products. *See* Ex. E (SW-SEC00298924); Ex. F (SW-SEC00006628). The cited documents are not inconsistent with the Security Statement.

1. November 2018 Slide Deck

13. I understand the SEC cites a slide in a November 2018 slide deck titled “FY18 Initiatives,” which contains a chart of various initiatives with notes on each. One row in the chart reflects an entry for “PEN Testing” with a note stating: “Unfunded in FY18. Plan to PEN test 8-10 products in 2019.” Ex. E (SW-SEC00298924 at -8934).

14. This note does not mean that SolarWinds failed to do penetration testing at the time. It refers to a specific budget request for *external* penetration testing—penetration testing conducted by a third-party provider, rather than penetration testing conducted internally by SolarWinds software engineers. External penetration testing requires budget allocated for that purpose to engage the outside vendor, unlike internal penetration testing that can be conducted with personnel on SolarWinds’ payroll. SolarWinds engaged external penetration testers to supplement the penetration testing we did internally. The fact that a particular budget request for external penetration testing went unfunded for FY2018 does not imply that no penetration testing at all was done in FY2018, as we would have been doing penetration testing internally. Moreover, the fact that this particular budget request went unfunded does not even mean that we did not do any *external* penetration testing for FY2018, as it could have been funded from a different source. In fact, we did do external penetration testing in FY 2018 for all of the Company’s MSP and Cloud products, as reflected in a slide deck from the time summarizing the results of the testing. *See* Ex. G (SW-SEC-00295588).

2. July 2020 Slide Deck

15. I understand the SEC cites a slide in a July 2020 slide deck that includes notes stating: “Inconsistent internal security testing as part of product final security reviews don’t always

include web application testing before release” and “Customers continue to actively engage 3rd party penetration testers as part of their compliance efforts.” Ex. F (SW-SEC00006628 at -6635).

16. The statement “Inconsistent internal security testing as part of product final security reviews don’t always include web application testing before release” simply indicates that Final Security Reviews being prepared by software development teams did not “always” include web application testing results, which could mean either that the testing was not being done in those instances or that the results were not being included in the Final Security Review documentation they prepared. The statement was not saying that the Company was generally failing to conduct such testing; it was merely flagging that our practices could be more consistent. Under the notation there are references to “Checkmarx” and “Whitesource”—two testing products used by SolarWinds—to remind employees that these tools were available for them to use for web application testing. These tools were in fact routinely used by development teams during the Relevant Period.

17. As for the statement “Customers continue to actively engage 3rd party penetration testers as part of their compliance efforts,” it simply indicates that some customers were conducting independent penetration testing of SolarWinds’ products as part of their own compliance programs. This is common in the software industry. It does not imply that SolarWinds was not conducting penetration testing itself.

C. Documents on Which the SEC Intends to Rely to Challenge the Security Statement’s Representations About Passwords

18. I understand the SEC cites an email I wrote in December 2020 about a security researcher’s report sent to us a year earlier concerning a SolarWinds password the researcher had found in an online code repository that had accidentally been made publicly searchable. *See* Ex. H (SW-SEC00407702).

19. In my December 2020 email, I wrote: “I have assumed this was our main download site. ... The point [the security researcher was] making was that they could have corrupted one of our downloads.” *Id.*

20. To clarify, I did not personally know whether the compromised password could be used to corrupt any of our downloads, i.e., to replace any of the products we made available to customers for download. I was only saying that this was a risk the security researcher was concerned about. My colleague, Lee Zimmerman, runs SolarWinds software release management program and is more knowledgeable on this topic than I am. I have reviewed his declaration and defer to his knowledge of the issue. *See Zimmerman Decl.* ¶¶ 2-10.


III. CONCLUSION

21. I would like to emphasize again that at all times throughout my tenure at SolarWinds, the policies in the Security Statement that are the subject of this lawsuit were true, and I believed them to be true. SolarWinds implemented each of the policies a regular practice, and I am not aware of any evidence of any pervasive failures to do so.

[*signature on following page*]

I declare under penalty of perjury that the foregoing is true and correct.

Executed on: April 25, 2025


Timothy Brown